Bachelor's thesis

Degree Programme in Industrial Management and Engineering

2020

Marko Merikko

WIRELESS MACHINE SAFETY TECHNOLOGY ANALYSIS

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Industrial management and engineering

2020| 54,1

Marko Merikko

LANGATTOMIEN KONETURVALAITTEIDEN VERTAILUANALYYSI

Tulevaisuuden tuotantolaitoksissa koneturvallisuuden merkitys tulee kasvamaan entisestään, kun itsenäiset järjestelmät ja koneet työskentelevät yhteistyössä ihmisten kanssa. Koneturvajärjestelmille asetetuista vaatimuksista tärkeimpiä ovat luotettavuus sekä vasteajat, jonka vuoksi järjestelmät ovat perinteisesti toteutettu käyttämällä langallisia viestintäkanavia. Langaton viestintätekniikka on lähivuosina kehittynyt merkittävästi, ja useilta eri valmistajilta on nyt myös saatavilla langattomia koneturvajärjestelmiä.

Tämän opinnäytetyön aiheena on langattoman turvatekniikan nykytilanteen selvittäminen sekä vertailuanalyysin tuottaminen. Tavoitteena oli tuottaa selkeä kokonaiskatselmus markkinoiden tämänhetkisestä tilanteesta kartoittamalla eri valmistajat, teknologiat ja tuotteet vertailuanalyysin avulla. Vaikka markkinoilla on jo paljon varteenotettavia tuotteita, uusia innovatiivisia ratkaisuja sekä kehitystä reaaliaikaisessa langattomassa viestinnässä tarvitaan vielä, jotta langattomat ratkaisut pystyvät kilpailemaan langallisten vaihtoehtojen kanssa.

ASIASANAT:

Koneturvallisuus, Teollisuus 4.0, Vertailuanalyysi

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme

2019 | 54,1

Marko Merikko

WIRELESS MACHINE SAFETY TECHNOLOGY ANALYSIS

As machines and production systems are becoming more intelligent and autonomous, functional safety will play a more important role in the future than ever before. Reliability and timeliness are the main requirements set for a safety control system, for which most safety control systems use wires as the signal transferring medium. In recent years wireless safety systems have become more reliable, and companies are now launching viable wireless safety products on the market. Wireless communication has many upsides compared to wired systems, and it is a fundamental requirement of future manufacturing systems.

The purpose of this thesis was to establish a comprehensive overview of the current state in the wireless safety market. This was done by using product benchmarking, mapping out different manufacturers, solutions, and products currently available on the market. It was established that there are viable wireless safety technologies available from multiple different manufacturers, but to fully harness the benefits of wireless communication in safety applications, new novel solutions, and advances in reliable real-time communication are still needed.

KEYWORDS:

Machine Safety, Industry 4.0, Benchmarking

CONTENT

FIGURES

LIST OF ABBREVIATIONS (OR) SYMBOLS

CCF	Common Cause Failure
DC	Diagnostic Coverage
DSSS	Direct Sequence Spread Spectrum
EAA	European Economic Area
EN	European standard (European Norms)
FHSS	Frequency Hopping Spread Spectrum
IEC	International Electrotechnical Commission
IoT	Internet of Things
IIoT	Industrial Internet of Things
ISM	Industrial Scientific Medical
ISO	International Organization for Standardization
$MTTF_d$	Mean Time To Dangerous Failure
M2M	Machine to Machine
PFH_D	Average Probability of Dangerous Failure per Hour
PL	Performance level
PLr	Required Performance Level
SIL	Safety Integrity Level

1 INTRODUCTION

This work was assigned by Schneider Electric Automation GmbH with its objective to investigate the current state of wireless safety technology on the machine safety market. The goal of this work is to create an overall view of the markets current state by mapping out the largest competitors and their products with selected benchmarking methods and evaluating future development of the market.

With the fourth industrial revolution around the corner machine safety will be in a more important role than ever before. Machines and systems are becoming increasingly independent, with capabilities to make decisions without human interaction. Ensuring a safe operating environment when humans are interacting with machines is going to be one of the major challenges of future manufacturing systems.

Wireless communication systems are a fundamental requirement of Industry 4.0 when considering their usability, scalability, and price. However, designing wireless safety architectures is challenging as the safety function must be ensured with a very low probability of system failure. This means that the system must have high standards for reliability and security. The applications must also have very low latency, as the initial time delay between the triggering event and the output function is required to be almost instantaneous.

1.1 Schneider Electric Automation GmbH

Schneider Electric SE is a global specialist in energy management and automation. In 2018, the company had more than 137,000 employees worldwide with a revenue of 25.7 billion. https://www.schneider-electric.com/en/about-us/company-profile/ Schneider Electric Automation GmbH is part of the Schneider Electric Group, developing and producing hardware and software products for advanced machine solutions. The global headquarters for machine solutions are in Marktheidenfeld, Germany, with approximately 500 employees from 26 different nations. (https://www.se.com/de/de/about-us/company-profile/standorte/marktheidenfeld-english-version.jsp)

2 THE FOURTH INDUSTRIAL REVOLUTION

There are three periods in time, where major advances in technology radically changed our way of producing goods. These periods have been defined as industrial revolutions. The first industrial revolution took place in the late 18th century when new steam-powered machinery sped up manufacturing processes that were previously carried out by hand production and moved production from home to factories. The second industrial revolution in the late 19th century introduced machines powered by electricity and mass production lines. The third industrial revolution took place in the 1970s when information technology and computers were integrated into manufacturing systems. (Muhuri P. K. & Shukla. A. K. & Abraham A. 2019)

The world is now on the brink of the fourth industrial revolution. Germany has set a strategic initiative in place, so-called “Industrie 4.0”, with its goal to boost industries productivity by 30% in the next 10 years, pushing companies to get ready for the new era of manufacturing. The goal of the program is to establish Germany as the market leader in industrial automation and advanced manufacturing applications, and other countries seem to be following their example. The future manufacturing systems are autonomous entities connected into a global network, where intelligent machines and production systems are operating and communicating with each other in real-time. These entities can make independent decisions based on real-time data and analytics and optimize manufacturing processes without human interaction. In future production systems, humans are only needed to monitor the overall systems performance instead of micromanagement and to carry out repairs and system maintenance that machines are not yet capable of performing. (Collin, J. & Saarelainen, A. 2016, 31-34)

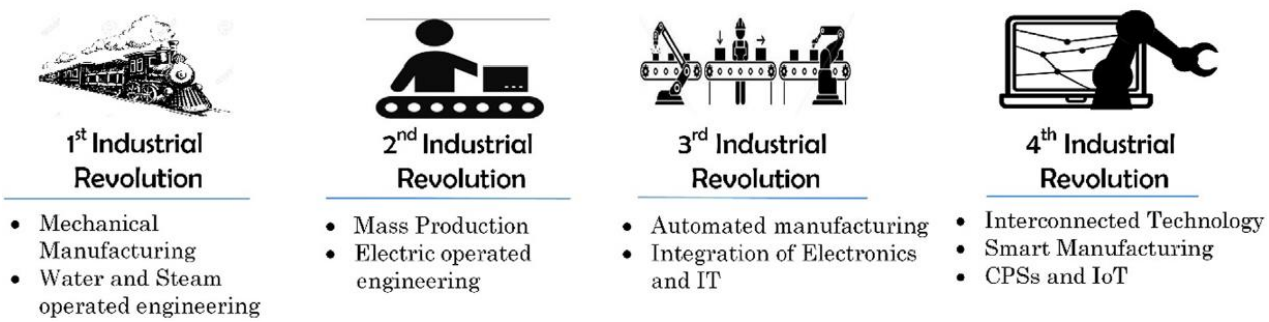


Figure 1. The fourth industrial revolution (Muhuri P. K. & Shukla. A. K. & Abraham A.)

2.1 The driving factors behind Industry 4.0

Information technology is once again revolutionizing industries. The vast improvements in processing power have been coupled with a dramatic drop in component prices and physical sizes. Products that have been traditionally seen consisting of two parts, mechanical and electrical components, are now becoming complex systems with multiple additional layers of complexity. These new “smart” products or systems are built by combining hardware, software, data storage, microprocessors, sensors, and connective elements. This development is enabling systems to be used in an increasingly effective way, bringing additional functionality and generating new added value for the user from the constant flow of information. This new way of system utilization is moving industry boundaries as well as creating completely new business opportunities or even industries. (Porter, M. & Heppelmann, J. 2014)

The main enabler of this development has been the new level of connectivity provided by the Internet of Things (IoT) or Industrial Internet of Things (IIoT). These terms are used to reflect the increasing number of connected objects within a system. However, these phrases can be misleading, as the internet is fundamentally only a way of transmitting information. The most significant factor is the data that is being generated by the connected objects and the ability to effectively gather and utilize it in meaningful ways. (Porter, M. & Heppelmann, J. 2014)

Sensors, communication modules, and software applications are now able to integrate analog physical entities with the digital world, providing constant information flow of the system. This information flow enables the system to perform real-time analytics and to make collaborative decisions and coordinated actions in a timely and accurate manner, creating a basis for a smart production system. (Chou S., 2018)

These new “intelligent” systems boost productivity in all manufacturing sectors when before purely physical systems and products will be able to generate and share digital data and cooperate with other systems. Because of this, the product and its tied services are bound to change, which will alter the whole value chain of the product. The new manufacturing systems require expertise in multiple different fields such as software development, cybersecurity and data analytics. To have the required level of expertise in these fields, companies must increasingly resort to external resources, as only a few manufacturing companies have all the required resources internally. Also, the new services

created require that companies form much stronger relationships with their customers than before, and the infrastructure must be able to support these new production methods. (Porter, M. & Heppelmann, J. 2014)

According to Cisco IBSG, more than 50 billion devices will be connected to the internet by 2020, with around 10 billion devices connected from the industry sector. A typical wireless sensor network (WSN) has a high number of sensor nodes, ranging from a few to tens of thousands. As the size of the sensor networks is rapidly growing, the pressure to move from wired to wireless solutions increases. Industrial wireless sensor networks (IWSN) offer a better alternative to wired sensor networks when the number of connected objects increases, as they can offer greater flexibility and expandability as no wiring is needed between the communicating objects. Installation times are also reduced as a result, and maintenance is made easier when the possibility of cable damage on the factory floor is removed. This also offers increased freedom when dealing with moving machinery. By utilizing IWSN, systems efficiency can be drastically increased in combination with reduced costs. (Wang, Q. & Jiang, J. 2016)

2.2 The four dimensions of a smart production system

Production systems capabilities can be described by four stages, with each step towards autonomy increasing the systems performance: monitoring, control, optimization, and autonomy. To achieve partial or complete autonomy, the system must be able to fulfill the requirements of each preceding level. (Porter, M. & Heppelmann, J. 2014)

2.2.1 Monitoring

The first level of performance is achieved when the system can gather data of its operations and external conditions that are present. This is achieved by installing sensors to the system that take given measurements in predefined intervals. External data sources may also be used for defining the external conditions. The most important design stage is deciding what needs to be measured and how the gathered data can be used to produce value for the company. When the sensors are used to measure meaningful information, the gathered data can then be used to make appropriate changes to the system or to track system performance. For example, if a machine is operated incorrectly, the deviations from optimal can be seen from the sensor data and feedback can be given to

the machine operators. Not only will sensors help in optimizing the production processes and machine lifetime, but many other internal departments may also benefit from the gathered data to boost their own processes. Market segmentation may benefit from analyzing usage patterns of the customers; logistics can be optimized with real-time data from production, after-sales services can benefit from the decreased machine downtimes enabled by advanced predictive maintenance and new customer needs may be identified by the sales department. The benefits of a carefully designed monitoring system extend throughout the organization. (Porter, M. & Heppelmann, J. 2014)

2.2.2 Control

The second level of performance is established when system monitoring is combined with controlling functions. This can be achieved through algorithms that steer the systems, reacting to sensor measurements in real-time. The controlling functions can be performed either by embedded software in the system or in the cloud by using so-called cloud computing, where remote server located elsewhere collects and processes the locally produced data. (Porter, M. & Heppelmann, J. 2014)

2.2.3 Optimization

Once the monitoring and controlling functions are in place, it becomes possible to optimize the system performance. With the modern data-storing capabilities, sensor data and system performance can be stored and tracked from longer periods of time. When this generated data is combined with algorithms and analytics, the system can self-optimize its processes. This will improve system utilization free resources to be used for other purposes within the company, as there is no longer a need for the personnel to perform manual analysis of the data. The costs of the system can be reduced when predictive maintenance can be performed with increasing efficiency. The systems conditions can be analyzed before its failure, and occurring trends or indicators can be found by comparing the failure resulting conditions with historical data. This enables the maintenance of the system before it reaches a failure state. Some problems can also be repaired remotely by adjusting machine controls or via software updates. Even if the failure requires on-site repair, accurate information on the failure and required items reduce the service costs. (Porter, M. & Heppelmann, J. 2014)

2.2.4 Autonomy

The final step is systems partial or complete autonomy. Autonomous systems can learn about their environment and self-optimize their processes without human interaction, who are only needed to perform system maintenance and to monitor the overall performance. The system can self-diagnose possible service needs, coordinate with other systems, and the whole entity is able to adapt based on the gathered information. This greatly improves the efficiency of the production system, as operations are run with more precision, and they require less personnel, which reduces the operating costs. This can also potentially have a positive effect on systems safety if the personnel are no longer required to operate in dangerous environments. (Porter, M. & Heppelmann, J. 2014)

3 MACHINE SAFETY

3.1 General information

Danger is always present within a dangerous system, whereas a risk defines the probability and scale of damage caused by a hazard. The purpose of machine safety is to ensure the safe use of machinery by either removing the dangerous element from the machine or by minimizing these involved risks by safe system design. Companies have moral and legal obligations ensure the safety of their personnel, which means that all the dangerous systems must be designed in accordance with the relevant legislation and safety standards. Besides moral and legal obligations, ensuring the safety of the personnel also benefits the company financially, as an accident can result in a substantial economic loss. The total cost of the accident for a company includes sick pay for the injured employees, lost production time, increase in insurance premiums, lost customers, and even potential loss of the company's reputation. Some protective devices can also have a positive effect on production efficiency, as the personnel are able to move more freely in the dangerous area. (Machine safety guide, Schneider electric)

The general principle of machine safety is that a dangerous part of a machine should only be accessible when the machine is in standstill. The system must also be designed in a way that unexpected or unintended machine activation is not possible when personnel or their body parts are in the dangerous area. The safe design can be achieved in various ways, and the focus is on reducing the risk levels as much as it is reasonably practical. For example, a table saw can be made safe by removing the blade, but it is not very practical considering the machines function. (Machine safety, Schneider Electric)

3.2 European standards for machine safety: A, B & C standards

The regulations regarding machine safety are enforced within the whole European Economic Area (EAA). These regulations are given out by the machinery directive. Before the new approach program was launched by EEC in the 1980s, the directive used to give detailed technical requirements for systems, but since the new approach, machine directive gives guidelines for safe machine design, as giving out technical requirements for every individual system would be hard, time-consuming and impractical. General

requirements for machine safety are set by the directives, which are completed with the machine safety standards. (Siirilä T. 2008, 25)

The standards designed to support the machine directive are categorized into three different levels, with each level giving out more detailed design principles for the system.

Type A standards specify basic concepts, terminology, and design principles which cover safe machine design requirements in general. These standards are applicable to all machines but are not detailed enough to be used as a standalone to ensure that all safe design requirements are met. (Siirilä T. 2008, 31-32)

Type B standards define requirements for one safety aspect or a safeguard that can be used in machines. The type B standards are divided into two subsections:

- B1 standards, which cover distinct safety aspects (e.g., noise, safe distance, temperature)
- B2 standards, which cover distinct safeguarding devices (e.g., emergency stops, interlocking devices, light curtains)

Type C standards are used to define detailed requirements for specific machines or groups of machines. These standards may come in several parts, with the first part of the standard series giving general requirements for the machinery group and the other parts giving requirements for specific machines. (Machine safety guide, Schneider Electric 2010)

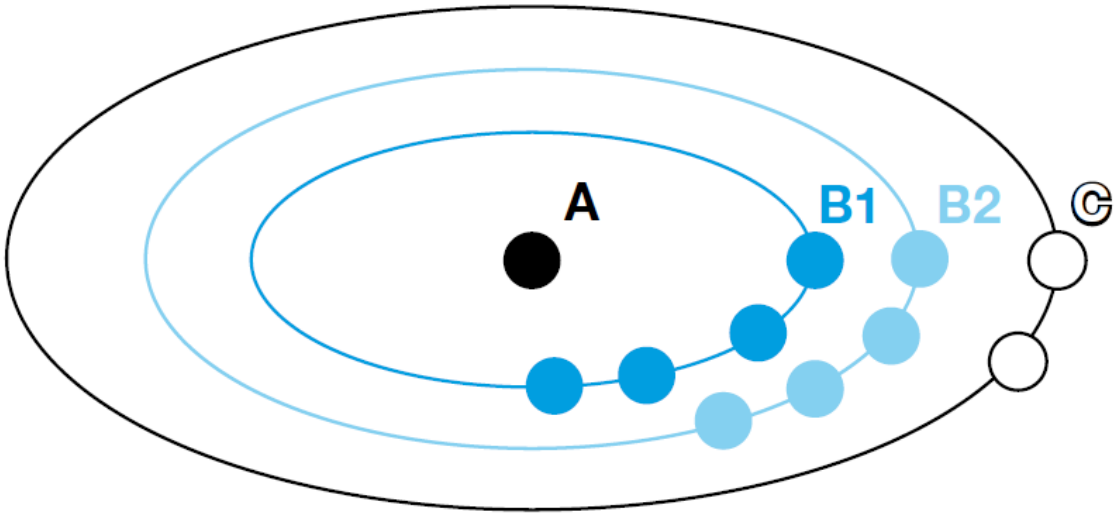


Figure 2. European standards for the Safety of machinery form. (Machine safety guide, Schneider Electric 2010)

3.3 General safe design principles

The machine directive sets a large variety of requirements for machine control systems. To summarize the main requirement set by the directive, the system must be designed so that even in the event of system failure the machine will not cause danger, which in practice means that the risk of failure must be minimized to an acceptable level. (Siirilä T. 2008, 78)

EN ISO 12100 gives general principles for risk assessment and risk reduction to achieve safe machine design. This risk assessment and risk reduction process follows a waterfall model, where each sequential step is completed before moving onto the next one. The first step of the process is to determine the limitations of the machinery. This means that all possible hazardous situations must be taken into consideration, which includes scenarios caused by the correct operation of the machine as well as any potential foreseeable misuse of the machinery. When all hazards are identified, a risk level is estimated for each individual hazard, which includes evaluating the severity of harm from the hazardous event and the probability of this given event. The final step is to take the needed actions to eliminate the hazard or to reduce the risk by means of protective measures. (Machine safety guide, SICK)

The objective of EN ISO 12100 standard is to achieve the greatest practicable risk reduction without hindering the performance of the machine. This means that the most important aspect is the safety of the machinery throughout its lifecycle, but also the ability of the machine to perform its desired function, usability and costs of manufacturing, operating and dismantling are considered. (Machine safety guide, Schneider Electric)

3.3.1 The three levels of risk reduction

Level 1: Hazard elimination or risk reduction by design

Removing the hazard or risk by design is the most effective way of ensuring machines safety. Even well-designed safeguarding has a probability of failure, whereas inherent protective measures are most likely to remain effective when the risk has been excluded

by design. This can be achieved by modifying the physical aspects of the machine itself or restricting the interactions between the person and the machine. (SFS-EN ISO 13849-1)

Step 2: risk reduction by safeguarding and possibly complementary protective measures

Guards and protective devices must be used when an inherently safe design is not possible or reasonably practicable. The choice of the safeguarding machine is made based on the machines risk assessment. These devices will be discussed in more detail in the following chapters. (SFS-EN ISO 13849-1)

Step 3: Information for use

An integral part of the safe machine design is to ensure that its users have identified the risks at hand. Information about the machine can be given out in the form of text, words, signals, signs, symbols, or diagrams. The information also needs to indicate if the machinery requires training, use of personal protective equipment or of the possible need of additional guard or protective devices. The goal is to inform the user about the intended use of the machine, accounting for all possible operating modes, and that it is understood by both professional and non-professional users of the machine. (SFS-EN ISO 13849-1)

Functional safety

Functional safety is a term used when the effect of a protective measure depends on a control system. The standards used for setting requirements for the safety-related control systems are EN ISO 13849-1&2 and IEC/EN 62061. These standards differ slightly in evaluating the overall safety of the control system. While EN ISO 13849-1 defines 5 different Performance Levels (PL) for systems, IEC/EN 62061 uses 3 Safety Integrity Levels (SIL). The ISO standard can be applied to pneumatic or hydraulic systems, where the IEC standard is not applicable. Fully programmable systems cannot be evaluated with the ISO standard, whereas the IEC standard can evaluate these systems. The machine builder can freely choose which standard to use depending on the application, and both standards share the same objective of focusing on the functional safety of the overall machine. (Siirilä T. 2008, 129-130)

As covering both standards would be excessive for this work, EN ISO 13849-1 will be used as the basis of the following chapters.

The first step of the risk reduction process is to perform a risk analysis, which will evaluate the required performance level (PLr) for the system. For the system to be considered safe, it needs to be designed in a way that it reaches this set performance level. The PLr of a system is evaluated based on the severity of the injury, average time on being exposed to the hazard, and the possibility of avoiding or limiting the harm. For example, if the machine is simple, and the risk reduction is based mainly on separating the danger area with barriers, the control systems impact for safety might not be significant. The control system is mainly required to ensure that the machine can be stopped with an emergency stop command (E-stop) and that the machine is unable to start unexpectedly. The control system has a high impact on the safety of the system when the danger area is not separated with physical barriers, and the safety of the system depends on detection devices or control equipment. When no barriers are between the danger area and personnel, the control system must always ensure safe stopping of the machine when personnel are entering the detection area, or control equipment is used. (Siirilä T. 2008).

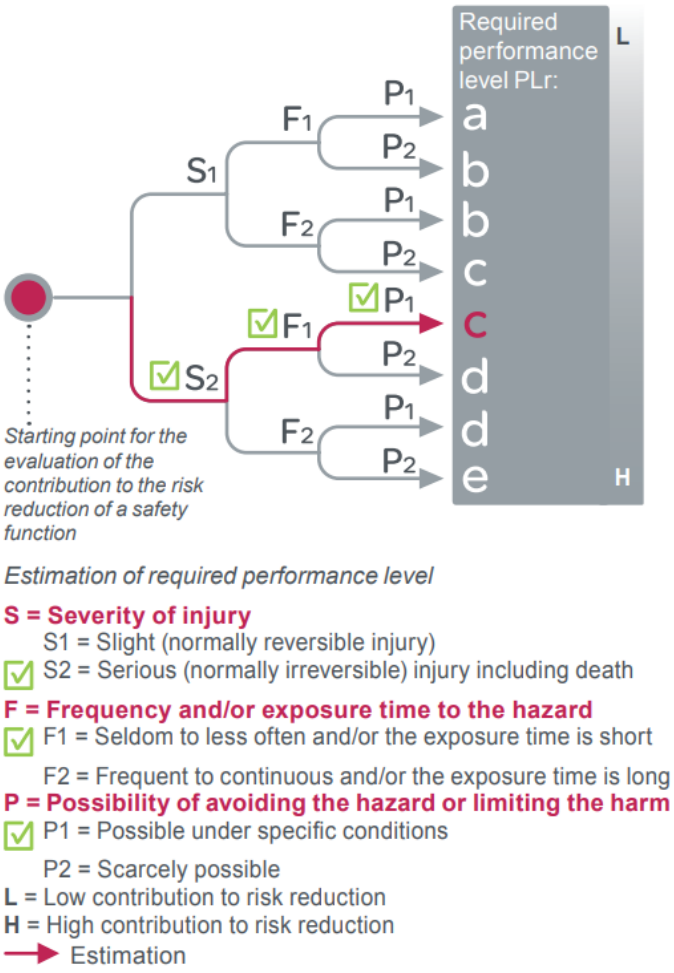


Figure 3. Graph for determining required PLr for safety function (SFS-EN ISO 13849-1:2015)

When the PLr is defined for the system, the system needs to be designed so that it complies with the requirements of the PL. The same PL can be achieved with different system architectures and components, which is described in detail in the ISO 13849-1 standard. To summarize, the control systems PL is calculated by evaluating its Diagnostic Coverage (DC), Mean Time To Dangerous Failure ($MTTF_D$), Category (Cat.) and protection against Common Cause Failures (CCF). This benefits the machine builder, as for example, the designer may use simpler circuitry when more reliable components are used to construct the system, and the safety circuit can be assembled with fewer components. In order to evaluate machine safety according to EN ISO 13849-1, software tools have been created that calculates the obtained PL of a system based on its subsystems, such as SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications). (Machine safety guide, Schneider Electric)

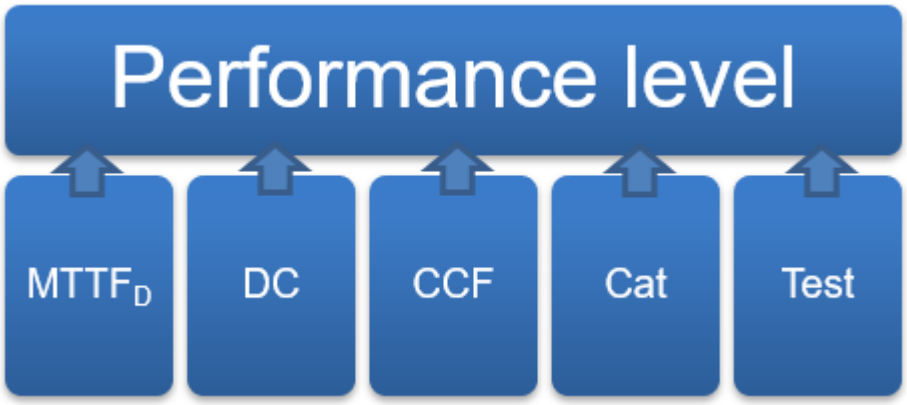


Figure 4. Defining performance level

3.3.2 Mean time to dangerous failure

One of the most important factors used to evaluate systems reliability is the likelihood of its components failing. The $MTTF_D$ value determines the average time for a component to fail dangerously. ISO 13 849-1 gives multiple possible methods that can be used when evaluating a components $MTTF_D$. The first method is to make an assessment based on the good engineering methods used when constructing the component. In principle, this means that the components are designed and manufactured using well-tried safety principles in accordance with the requirements set in ISO 13 849-2. The second method that can be used is determined in Annex C5, where a list of approximate $MTTF_D$ values for different electrical components are given. For mechanical, electromechanical or pneumatic components, the MTTFD can be calculated with the mean number of annual

operations (N_{op}) and the number of cycles until 10% of the components fail dangerously (B_{10D}). (SFS-EN ISO 13849-1)

$$\mathrm{MTTF_D} = \frac{B_{10\mathrm{D}}}{0{,}1 \times n_{\mathrm{op}}}$$

Equation 1. Formula of MTTFd (SFS-EN ISO 13849-1 2015)

The standard uses a 3-level scale on evaluating the reliability of systems channels, with the maximum achievable value being 100 years. This value is limited so that the component reliability is not overstated in comparison with other influencing variables to a control systems safety, such as the architecture or testing. For Cat.4 subsystems, the maximum value of MTTFD is set to 2500 years. (ISO 13849-1:2008)

$\mathrm{MTTF_D}$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $\mathrm{MTTF_D}$ < 10 years
Medium	10 years ≤ $\mathrm{MTTF_D}$ < 30 years
High	30 years ≤ $\mathrm{MTTF_D}$ ≤ 100 years

Figure 5. Mean time to dangerous failure of each channel (SFS-EN ISO 13849-1 2015)

3.3.3 Diagnostic coverage

The diagnostic coverage describes the control system's ability to detect failures within its subsystems. When designing a safety function, it must be taken into consideration that the control system's components and the software will have faults in them. The system must be designed in a way that these faults are discovered before they have an influence on the safety function. When a fault is detected, it usually results in controlled stopping of the machine in systems with zero fault tolerance. The system must also be designed in a way that prevents the machine from starting before the fault has been eliminated. If this aspect is not carefully considered in system design, it will result into dangerous failures, which includes failures that will result in loss of the safety function or failures that the diagnostics of the system is unable to detect. (SFS-EN ISO 13849-1)

ISO 13849-1 gives estimates on the diagnostic coverage achieved for different input, logic, and output functions. Often control systems use several different methods for fault detection, and these different methods often have different values for DC. The systems total diagnostic coverage (DC_{avg}) is calculated with the following formula, where each individual blocks DC and $MTTF_D$ are taken into consideration:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

Figure 6. Estimation of average DC (SFS-EN ISO 13849-1 2015)

The systems resulting DC_{avg} is factored in when determining the PL or SIL achieved for a system. ISO13849-1 defines 3 key threshold values for DC, 60% for low, 90% for medium, and 99% for a high level of DC. A DC_{avg} below 60% is not factored in, as it doesn't have a significant effect on the control systems reliability. (ISO 13849-1:2008)

Diagnostic coverage (DC)	
Denotation	**Range**
Nil	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

Figure 7. Diagnostic coverage (SFS-EN ISO 13849-1 2015)

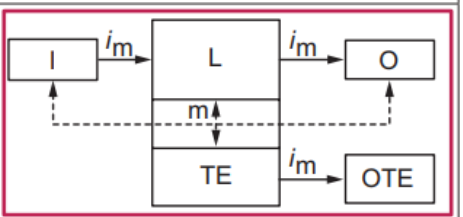
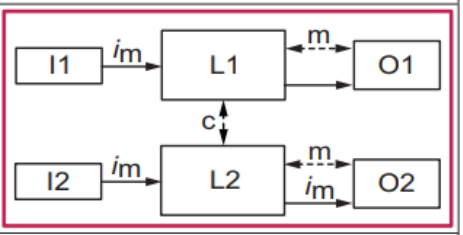
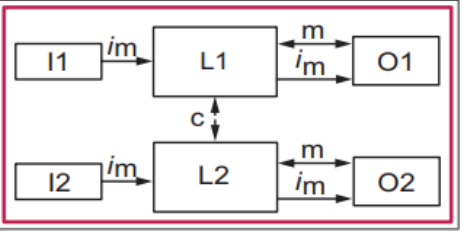
3.3.4 Common cause failures

A common cause failure is a failure, where one fault will influence multiple components or subsections of the control system. If a high-performance level is desired, the control system must be designed in a way that it has an acceptable level of protection against common cause failures. ISO 13 849-1 presents different methods for eliminating common cause failures, and it uses a numeric scale on evaluating the importance of different design principles. A control system must achieve a minimum total score of 65 points out of the possible 100 to be considered protected. The most important measures are a

physical separation between signal paths (15 points), the use of different technologies and diverse design principles (20 points), protection against environmental factors (35 points) and protection against over-voltage, over-pressure, etc. (15 points). (SFS-EN ISO 13849-1)

3.3.5 Categories

The ISO 13 849-1 defines 5 possible categories for the safety-related part of a control system, with higher categories increasing the reliability of the system. Safety categories define the behavior and safety of the system in the event of a fault. Cat. B&1 systems safety is ensured only by the reliability of its components when category 2-4 systems are more defined by their designated system architecture, and the safety function is assured even in the case of a single fault with redundant channels and diagnostic coverage. (SFS-EN ISO 13849-1)

Cat.	System behaviour	Designated architectures
B	A fault can lead to loss of the safety function	
1	As for category B but the probability of this occurence is lower than for the category B	
2	A fault can lead to loss of the safety function between two periodic inspections and loss of the safety function is detected by the control system at the next test.	
3	For a single fault, the safety function is always ensured. Only some faults will be detected. The accumulation of undetected faults can lead to loss of the safety function.	
4	When faults occur, the safety function is always ensured. Faults will be detected in time to prevent loss of the safety function	

Key:

*i*m: Interconnecting means
c: Cross monitoring
I, I1, I2: Input device, e.g. sensor
L, L1, L2: Logic
m: Monitoring
O, O1, O2: Output device, e.g. main contactor
TE: Test equipment
OTE: Output of TE

Figure 8. Category representation (applying SFS-EN ISO 13849-1 2015)

Category B: Relevant standards and basic safety principles are followed. There is no DC within category B systems, and the MTTFd can be from low to medium. CCF doesn't have to be considered, as a single fault will result in the loss of the safety function. Cat. B systems can reach up to PL b. (SFS-EN ISO 13849-1)

Category 1: System is constructed by using well-tried components and well-tried safety principles, which means that the components have been used successfully in the past in similar applications or they've been verified to be suitable and reliable in safety-related applications. Category 1 systems can reach up to PL c. (SFS-EN ISO 13849-1)

Category 2: The safety function is tested by the control system in suitable intervals, at machine start-up, and before it is used in any hazardous situation. The machine can only be operated if no faults are detected by the test channel, which must be able to reach DC_{avg} above 60%. Cat. 2 systems can reach up to PL d. (SFS-EN ISO 13849-1)

Category 3: System must be designed in a way that a single fault will not result in loss of the safety function, which means that redundant channels are implemented. The DC_{avg} of each channel must be able to reach a minimum of 60%. The $MTTF_D$ of each channel must be from low to high, depending on the required PLr. Measures against CCF must be applied. Faults will be detected when reasonably practical, but the accumulation of undetected faults can still lead to a loss of the safety function in Cat. 3 systems. Cat. 3 systems can reach up to PL d. (SFS-EN ISO 13849-1)

Category 4: Faults are detected on time before the next demand of the safety function and accumulation of undetected faults will not result in the loss of the safety function. The resulting DC_{avg} must be above 99%, and $MTTF_D$ of each channel must be high. Measures against CCF are considered in the design. Cat. 4 systems can reach up to PL e. (SFS-EN ISO 13849-1)

3.3.6 Evaluating achieved safety levels

When the required performance level has been set, it can be achieved with multiple different variations of MTTFD, DC_{avg} and Category. In combination with the PL and SIL, Probability of Dangerous Failure per Hour (PFH_D) is used to describe the overall reliability of a control system. An illustration of the achieved PL and PFHD according to ISO 13

849-1 is presented below. The graph gives a rough estimate of the control systems achieved PL and PFHD, as well as a visual representation of the relationships between different Categories, $DC_{avg,}$ and $MTTF_D$. Accurate values can be found in the ISO 13 849-1 standard. (Machine safety guide)

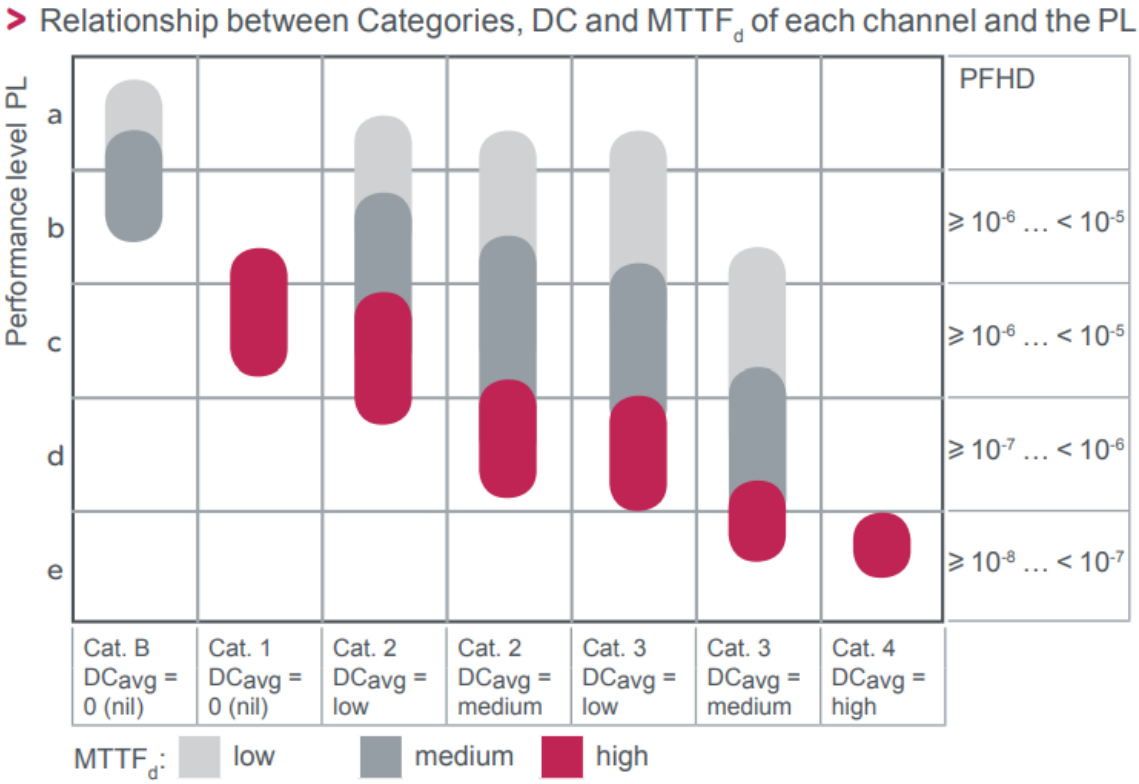


Figure 9. Relationship between Categories, DC and MTTFd of each channel and PL (applying SFS-EN ISO 13849-1 2015)

IEC/EN 62061 uses slightly different methods for evaluating the reliability of a system, which means that SIL and PL are not directly comparable. However, the two standards are closely related, and the correspondence between PL and SIL can be established through the probability of dangerous failure per hour, which is defined in both standards. Below is an illustration of the correlation between SIL and PL based on their assigned PFH_D values. (Machine safety guide, SICK)

PL	SIL	Probability of dangerous failures per hour 1/h
a	No correspondance	$\geq 10^{-5} \ldots < 10^{-4}$
b	1	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$
c	1	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$
d	2	$\geq 10^{-7} \ldots < 10^{-6}$
e	3	$\geq 10^{-8} \ldots < 10^{-7}$

Figure 10. Relationship between PL and SIL (applying SFS-EN ISO 13849-1 2015)

The two standards are slightly mismatched on the PFH_D scale, as PL a doesn't have correspondence in the SIL scale, and SIL 4 doesn't have correspondence in the PL scale. SIL 4 is not generally displayed in the graph in a machine safety context, as it is overly demanding for machine safety applications in general. (Machine safety guide, SICK)

3.4 Design of a safety function

The safety function defines how risk is reduced by using protective measures. If a hazard cannot be eliminated by inherently safe design, it must be assigned an appropriate safety function that will reduce the risk to an acceptable level. The hardware components used to build a safety-related control system can be divided into three different subcategories: input, logic, and output devices. (Siirilä T. 2009, 101-104)

These are components that have been manufactured according to the relevant machine safety legislation and standards, and certain components need to be certified for them to be used in the safety-critical application. A minimum of 1 sub-system from each category is needed when designing the basic structure for a safety-related control system.

The needed safety components are dependent on the application where they will be used. The required safety level of the system can be established with various architectures, and multiple possible solutions are usually available to achieve the same desired outcome. A division can be made based on how the components operate and detect dangerous situations. Different physical principles can be used for detection, and one detection method is not applicable to everything, as it may be insufficient in monitoring the danger area, subject to environmental interference or not practical in other ways considering the application. (Siirilä T. 2009, 101-104)

3.4.1 Acquiring information (input)

Guards

Guards are protective devices used to prevent the machine operator from directly reaching the hazardous area of the machine. This can be achieved, for example, through covers, barriers, fences, or doors. Besides preventing access to the hazardous area, guards can be used to protect the operator from dangerous ejected materials or radiation produced by the machine. Depending on the application, guards are either mounted or movable. When guards are not frequently opened, mounted guards are preferred. This means that the guard can be only removed with tools when access to the hazardous area is needed. If the hazardous area needs to be accessed frequently, movable guards are used. In these cases, it must be made sure that the guard can perform the desired safety function. (Machine safety guide, SICK)

Figure 11. (Safety switch, Schneider Electric 2018)

Electro-sensitive protective equipment (ESPE)

With electro-sensitive protective equipment, the protection is not established through physical separation of the operator and the machine, but by monitoring the entrance to the danger area and sending a stop command when it is accessed. This must be done in a way that detection is in time for the machine to fully stop before the hazardous area is possible to enter, which means that ESPE can’t be used with a machine that has long run-down times. This is beneficial in situations where the operator must regularly access a machine, as it can be done without the need of opening a guard. This reduces access

time, increases productivity, and improves workplace ergonomics. Detection can be established by using different principles, e.g., optical, ultrasound, microwave, infrared, or capacitive sensing. The most common ESPE devices are optoelectronic devices. (Machine safety guide, SICK)

Figure 12. (Safety light curtain, Schneider Electric 2018)

Position fixing devices

The purpose of a position fixing protective device is to ensure that the operator is outside of the hazardous area while operating the machinery. This is achieved by using a control device that is in a fixed position outside of the danger area. Most common position fixing device is two-hand controller, where two handles need to be continuously pressed with both hands to enable machine movement. In order for the position fixing device to be effective, the dangerous operating area should be entirely visible from the operating position, and the distance to the danger area should be long enough for the operator to be unable to reach it when the machine is still in a dangerous state. The position fixing device needs to have a complementary protection device close to it, typically e-stop, to stop the machine movement in case of an unexpected fault in the control device that prevents the machine movement to be stopped. Machine safety guide, SICK)

Figure 13. (Two-hand control station, Schneider Electric 2018)

Enabling devices

Enabling devices are control devices that can be used to enable machine movement when the danger area must be accessed while the machine is operated. For example, in some applications, the danger area of the moving machine is so large that restricting operators access to the whole area would not be practical. Instead, safety is ensured by forcing the machine operator to control the machine movement with an enabling device. This is established by making sure that the operator acknowledges the dangerous situation and can react to it in time. The enabling device is often used in combination with another controlling device, or it can be used as a standalone, e.g., during machine maintenance, setup, or process observation. (Machine safety guide, SICK)

Figure 14. (Enabling switch, Schneider electric 2018)

Machine parameter monitoring devices

Sensors monitoring machine parameters can also be used to ensure safe operating conditions. In safety-related applications, these sensors are mainly used to measure machines movement or position to ensure that the machine is not exceeding the set boundaries. In safe position monitoring, the moving part of the machine is monitored so that it remains in a specific area or at a certain position. The sensors can also measure, e.g., speed, pressure, temperature, or any other parameter that is relevant to the machine's safety. (Machine safety guide, SICK)

Pressure-sensitive equipment

Pressure-sensitive devices are used to stop or slow down machine movement when a person is detected in the danger area. The application should be designed in a way that the danger zone cannot be accessed without activating the pressure-sensitive device. Pressure mats and edges are the most commonly used pressure-sensitive devices. (Machine safety guide, SICK)

Figure 15. (Safety mat, Schneider Electric 2018)

Complementary protective measures

Complementary protective measures are protective measures that are designed to minimize the damage in the event of a hazardous situation. These measures should always be implemented in combination with other protective measures, even if the machine has inherently safe design or technical precautionary measures. The most important

complementary protective device is an emergency stop button, which will initiate the stopping of the machine. In general, all machines and working stations are required to have an emergency stop button. (Machine safety guide, SICK)

Figure 16. (Emergency stop button, Schneider Electric 2018)

3.4.2 Monitoring and processing (logic)

The signals from safeguarding components are monitored by using

Safety relay modules are the simplest and most affordable solution for small scale applications. They can monitor a single safety function, which means that if an application has, for example, two input devices, two separate safety modules are needed. Safety modules are usually preferred in small scale applications, but as the size and complexity of the application grows, more sophisticated devices are needed. (Schneider Electric. 2018)

Figure 17. (Safety module, Schneider Electric 2018)

Safety controllers are designed for more demanding, medium-sized applications. They can handle multiple safety functions at a time and are usually expandable with extension modules so that they can be modified to meet the needs of the application at hand. Safety

controllers can be configured by software, but they are not freely programmable. (Schneider Electric. 2018)

Figure 18. (Safety controller, Schneider Electric 2018)

Safety Programmable Logic Controllers (safety PLC) are designed for the most demanding safety applications. They can handle large-scale and complex applications where a high amount of safety devices are needed. Safety PLCs are freely programmable and configurable to meet the demands of the application. (Schneider Electric. 2018)

Figure 19. (Safety PLC, Schneider Electric 2018)

3.4.3 Stop the machine (output)

Contactors

Contactors are the most commonly used devices for power control. The function of a contactor is to simply remove power from machine actuators, ensuring that no torque generating energy can affect the motor. This also prevents the machine from starting unintentionally. Contactors are used in simple applications, where no special requirements are needed for the stop function, and the machine can freely stop until it reaches a standstill. (Schneider Electric. 2018)

Figure 20. (Contactor, Schneider Electric 2018)

Drives

Drive technology is used when a controlled stop is required by the safety application, for example, if the machine has high inertia, and the rundown time is long. With drives, the user has more control over how the stop will be initiated, instead of simply removing power from the machine actuators. (Schneider Electric. 2018)

Figure 21. (Variable speed drive, Schneider Electric 2018)

4 WIRELESS COMMUNICATION IN INDUSTRIAL APPLICATIONS

4.1 Radio transmission

Radio waves are part of the electromagnetic spectrum, and data transmission can be achieved with a broad range of different frequency bands. Each frequency band has its own properties with its own advantages and disadvantages, and the radio wave spectrum generally refers to electromagnetic frequencies between 10 kHz (kilohertz) to 3000 GHz (gigahertz). Communication with radio waves has an important differentiation to wired communication, as radio waves have a spherical propagation from the source, whereas in wired networks the signal only travels along the wire. If the wire is not damaged, it typically has the same characteristics at all points, and the behavior of the signal can be accurately determined. When transmitting wirelessly, the signal is subject to, e.g., environmental conditions, objects in the signal path, and interferences. This makes it harder to determine how the transmitted signal is going to behave. (Mobile communications)

The main issues caused by the environment are attenuation and multipath propagation. Attenuation causes the signal strength to weaken as the distance increases regardless of the interactions that it has with the environment. Because of the spherical propagation from the source, the intensity of the waves decreases according to the inverse square law meaning, e.g., that an object twice as far only receives one-quarter of the energy. In multipath propagation, the receiving device gets multiple copies of the originally sent wave, as the electromagnetic wave propagates to all directions from the transmitter and the waves are reflected or scattered by objects. (Wireless safety guide, Pepperl-fuchs)

Radio waves in free space are moving in an almost straight line like visible light, but very seldom there is a line of sight between the communicating devices. Radio waves can penetrate some objects, and generally, the lower the frequency is, the higher the penetrability. However, radio waves cannot penetrate metals, which is an important factor to consider in industrial environments. Besides the static objects that can be in the signal path, moving equipment, vehicles, and unconsidered installations may influence the communication. (Wireless safety guide, Pepperhl-fuchs)

Collisions and interference are also affecting the communication link and need to be considered in wireless communication systems. When two electromagnetic transceivers transmit at the same frequency at the same time, the signals might collide. This interfering signal can be from another transmitting device that belongs to the system (collision), or it can be from an outside source (interference). The source can also be an electromagnetic emission that is not intended to convey information (noise), for example, energy radiated from the operated machinery. Collisions can be avoided when the network controls how the channel is used. In other words, it needs to be deterministic. For example, Bluetooth and WLAN devices can coexist without interference when the Bluetooth device avoids the frequencies used by WLAN and only hops on the free frequencies. Interference can be dealt with to an extent by using different robust signal transmitting techniques. (Echoring, wireless propagation effects and their impact on reliable transmissions. [Referred 19.05.2019])

The radio wave doesn't contain information by default. The process of coding information to radio waves is called modulation. Information can be added to the radio wave by having a steady carrier signal, where the signals amplitude, frequency, phase, or other aspects are modified. This received signal is then demodulated by the receiver to retrieve the sent data. As the modulation techniques have got better over time, the quality of the communication link has increased. There are multiple viable modulation techniques, with the two most popular methods being frequency spreading techniques: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). As the name implies, in frequency spreading techniques, a narrowband signal is spread to a larger bandwidth. This has several advantages, with the most important one being resistance to narrowband interference. (Wireless safety guide, Mobile communications)

In DSSS, the original data is divided and simultaneously transmitted on many frequencies within a defined frequency band. The data is multiplied with a spread key, which means that an XOR is performed to the user bitstream and redundant bits are added, known as chips. The ratio between the chips and data is known as the spreading ratio. The higher the ratio is, the more immune the signal is to interference as the data can still be recovered with the remaining chipping code if the number of corrupt bits is not above a set threshold. The sent data can only be retrieved when the receiver has the same spread key to decode the message. DSSS is used, e.g., by ZigBee. (Mobile communications)

In FHSS systems, the used bandwidth is divided into multiple different channels. The signal is then sent in small parts by hopping from one frequency to another, where the transmitter and receiver are constantly changing between the channels, thus using the whole total available bandwidth. The receiver must know the hopping sequence and stay synchronized throughout the transmission to receive the transmitted signal successfully. In fast hopping systems, the transmitter changes frequency multiple times during the transmission of a single bit. This makes it highly resilient against narrowband interference. FHSS is used, e.g., by Bluetooth. (Mobile communications)

Network topology defines how the nodes are arranged in a communication network and how connections are established. A point-to-point connection is the simplest network topology, where a communication link is established between two endpoints. When the communication chain has more than two participants, the participants can be organized in multiple different ways. Most used types are mesh, star, and hybrid networks. In star networks, each end object communicates with the central coordinator, which collects and sends the data forward. The biggest benefits of a star network are the low latency as there is a direct connection between the endpoint and the gateway, devices can be added or removed without affecting other parts of the network and if one node stops functioning the other connections are not affected. In mesh networks, each end-point acts as a router, sending or receiving data from other sensors or from the coordinator, and all objects within range can communicate with each other. This can potentially offer redundant channels for communications that lower the risk of transmission failure but increases latency as the packet hops through multiple devices. Hybrid topologies combine aspects from both networks. (Wireless safety guide, Pepperl-Fuchs)

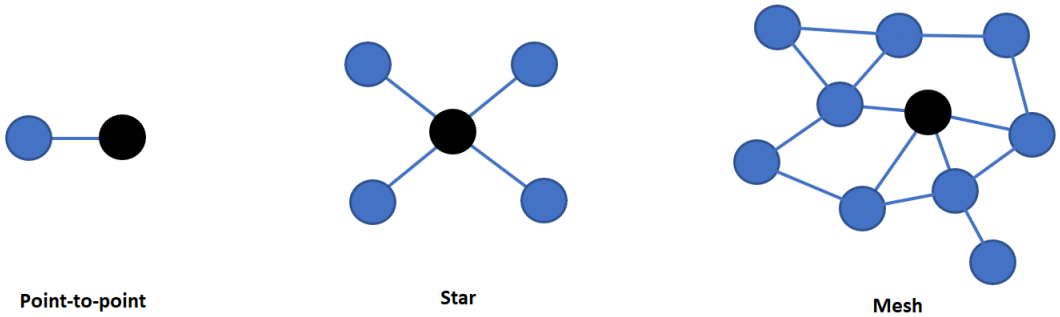


Figure 22. Illustration of example network topologies

4.2 Overview

Radio technologies are used worldwide in various applications. As radio frequencies are a finite resource, they are regulated both nationally and internationally. On a global scale, the spectrum use is coordinated by the International Telecommunication Union (ITU), and in Europe by the Conference of Postal and Telecommunication Administrations (CEPT). However, the final decision rests on national governments. In the EU, all electrical equipment must also comply with the low voltage directive and electromagnetic compatibility directive. The radio equipment must also be capable of using the radio spectrum efficiently and effectively. Some frequency bands are free to use by anyone without applying for a special license. These are called Industrial Medical Scientific (ISM) bands. The two most common ISM bands are located at 800-900MHz and 2.4 GHz. (Etsi, radio technologies [Referred 18.05.2019])

There are multiple valid options when building an industrial communication network. There is a wide variety of different data transferring methods, communication protocols, and standards, which allow data to be transferred from a machine to the information system or to other machines. In theory, it would be ideal to use as few different technologies as possible, but in practice, multiple different methods are needed for different applications. A variety of different communication methods are usually needed in large production systems, which causes problems in controlling the system as well as with updating, system compatibility, and overall functionality. These problems are tackled with gateway solutions, where the information flow is concentrated in a node, and the gathered data is sent forward in a unified form. (Collin, J. & Saarelainen, A. 2016)

When deciding the appropriate communication method, an assessment must be made of the whole operational environment and the need for transition in the future. A clear technical border is between wireless and wired systems. For some, the whole communication system is built on wireless networks, and others use mainly wired solutions. As wireless systems are constantly improving and have multiple benefits over wired systems, it is predicted that most of the new communication systems used in the future are wireless. The main advantage of a wireless system is the ease of scalability when physical wires are not needed between the communicating objects. (Collin, J. & Saarelainen, A. 2016)

If a data package is lost in a regular non-industrial application, it is just sent again, and it doesn't have a major effect on the functionality of the system. It only becomes noticeable if a majority of sent packages are lost, as this will slow down the communication speed. When considering industrial applications, especially safety applications, reliability and timeliness of the transmission are the main requirements set for a system. Rapid updated rates are usually not needed, but the arrival of the data packets must be ensured, as the failure to send packages can lead into interruption of the processes or even to a potentially hazardous situation. (Wireless safety guide, Pepperl-Fuchs)

Most industrial wireless communication systems operate in the 2.4GHz ISM band, as it license-free and IEEE 802.11-based infrastructure has become commonplace in production facilities. Designing the system to be compatible with these standards helps with managing and operating the whole facility. However, this might be problematic in the future if the bandwidth becomes too crowded, as the amount of interference caused by other communicating objects increases. (Collin, J. & Saarelainen, A. 2016)

4.3 International standards

Wireless Local Area Network (WLAN)

The first version of the IEEE 802.11 protocol was established in 1997, which was followed by IEEE 802.11b in 1999. Since then, there have been many revisions of this protocol, and new versions are constantly under development. There are several different wireless LAN technologies, but the term WLAN is often used as a synonym for IEEE 802.11 standard family. The big advantage of WLAN is that it follows the standards and topology of the Ethernet network. Up till recently, the main issues of using WLAN in industrial applications were the networks high power consumption and the weak signal penetrability of structures. However, a new 802.11ah standard (WiFi HaLow) was introduced in 2017 and has been developed for IoT and M2M usage in mind. It has a low power consumption, ranges up to 1000 meters, support for a large number of objects in a network, and M2M communication. The protocol also has a higher capability to penetrate objects, and it uses frequencies below 1 GHz when previous WLAN standards operated at 2.4 and 5 GHz. (Collin, J. & Saarelainen, A. 2016)

Bluetooth Low Energy (BLE)

Bluetooth low energy (BLE) is the optimized, low energy variant of the Bluetooth protocol. Its goal is to reach low power consumption in combination with high performance. BLE also offers compatibility with a broad range of mobile devices and Internet Protocol (IP). BLE transmits in the 2.4 GHz ISM band and uses frequency hopping. Transmission ranges usually vary between 10 - 100 meters depending on the transmitters power and operating conditions. BLE supports three different network topologies: point-to-point, broadcast, and mesh.

(Bluetooth Low Energy (LE) [Referred 18.06.2019])

IEEE 802.15.4

The IEEE 802.15.4 standard was designed for low power, low cost, and low data rate applications. However, it cannot be applied for harsh industrial applications, as it is not capable of dealing with noise and interferences to the required extent, but it serves as the underlying base standard for many other standards such as ZigBee, ISA100.11a, and WirelessHART which use its medium access control and physical layers. (Collin, J. & Saarelainen, A. 2016)

ZigBee PRO

The ZigBee PRO is a low power WSN standard founded in 2007. It is a revision of the ZigBee standard from 2004. The ZigBee standard was based on the IEEE 802.15.4 protocol, which meant that it operated on only one frequency defined by the user. This meant that the network was vulnerable to interference from other networks operating on the same frequency and other noise in the channel, and it wasn't considered to be performing on the required level in harsh industrial conditions. The ZigBee PRO specification was created with industrial applications in mind, and it has added security features as well as frequency agility, making it more resistant to noise and interferences. The network operates at 2.4Ghz frequency worldwide, with the possibilities to use 868MHz in Europe and 915MHz in North America. The network can transmit on a range from 10 to 100 meters depending on power output on 2.4GHz, and the frequencies below 1GHz are capable of ranges up to 1km. (What is Zigbee? [Referred 4.5.2019])

WirelessHART

WirelessHART enables wireless transmission of the Highway Addressable Remote Transducer (HART) field communication protocol. WirelessHART is based on the IEEE 802.15.4 protocol, but the physical and medium access control layers have been modified to allow frequency hopping. The standard operates in the 2.4GHz ISM band. The network has a different topology, and it uses a flat mesh network, where all radio devices operate simultaneously as a signal source and a repeater. This can potentially provide redundant signal paths, as the device can use multiple alternative routes to transmit the message to the end receiver. (Collin, J. & Saarelainen, A. 2016)

ISA100.11a

ISA100.11a is a standard based on IEEE 802.15.4 but with adaptations to enable frequency hopping, and it has set in place additional security mechanisms. It operates at the 2.4GHz ISM band and is designed to coexist with other IEEE radios. It supports start/mesh/hybrid network configurations and has redundant communication links with duocast. ISA100.11a uses IPv6 addressing and is compatible with 6LoWPAN.

(ISA 100, Universal Industrial Wireless Network [Referred 10.6.2019])

5 BENCHMARKING

Benchmarking is a tool used to measure organizations' performance in a selected area. It is a continuous process of comparing products, services, processes, or outcomes in a systematic manner to improve the company's products and processes by identifying and implementing best practices from competitors. When a company successfully implements continuous benchmarking as a part of the company's product development cycle, it will be able to identify innovative solutions already existing on the market and find problem areas in their own products and processes more effectively. Benchmarking can be used to determine areas that require improvement, providing valuable information when setting future goals and targets as well as with formulating company's plans and strategies. This also enables more efficient distribution of available resources. (Rowena Scott)

The use of benchmarking helps organizations in mapping out their core strengths and weaknesses. Organizations can more accurately determine their position in the market when the key differences between products and processes are documented, as well as the reasons behind them. Overall performance can be determined based on this information, giving a better idea of the organizations' current state and position in the market. This established knowledge can be used in setting new standards and objectives to steer product development. These new ideas gathered from outside of the organization can give fresh perspectives, which in turn speeds up innovation. Overall, benchmarking is a highly cost- and time-efficient way of establishing new innovative ideas which can be utilized in product development. This will improve the company's competitiveness and help in meeting the customers' requirements regarding product quality, cost, and service. (Metin Kozak, 20-23)

5.1 Benchmarking types

The main separation between different benchmarking methods is between internal and external benchmarking. The main process is initially the same for all the different benchmarking methods, and the difference lies mainly in determining the benchmarking subject and to whom will it be compared. The subject of the benchmarking process can be, for example, a product, strategy, function, or process. When the subject has been

decided, the organization needs to identify the most fitting partner to reach the best results. This can be either an internal or external organization. For example, another plant or department within the same organization, or direct competitor, industry leader or non-commercial organization. (G. Anand, Rambabu Kodali)

Internal benchmarking

Internal benchmarking means comparison that is conducted within the organization. It is two-way communication between different organizational parts, for example, between two similar departments. The benefit of internal benchmarking is complete and easy access to information, which gives the organization quick presentable results. Making performance comparisons is also simpler when the organization most likely has a common culture and systems in place. When an organization first compares the best practices used within the organization, it creates a baseline that helps with performing external benchmarking. Searching for better performance indicators in house and learning on how they are achieved is a valuable benchmarking tool, but the clear downside is the lack of fresh perspectives or innovations. (Metin Kozak, 28)

External benchmarking methods

Competitive benchmarking

Competitive benchmarking means comparing organizations performance with its direct competitors. It is defined as the most sensitive benchmarking method, as it is difficult to achieve healthy cooperation with organizations competing for the same customers. Organizations want to protect their practices, which allow them to achieve a competitive edge over other companies in the same industry. Gathering complete information or finding accurate sources can be extremely difficult, and often, the comparisons must be made with incomplete information. However, comparing the direct competitor's performance has the biggest upside, as it often offers new perspectives and increases sensitivity to change, creating a culture of thinking outside of the box. The organization can evaluate how effective its products and practices are compared to its competitors and improve to achieve excellence, adapting the best practices from industry leaders. The disadvantages of competitive benchmarking are the difficulties of obtaining information or applying the learned practices. Another risk might be developing the tendency of focusing on the aspects that make the main competitors distinctive instead of trying to develop better practices that would achieve higher performance. (Metin Kozak, 29-30)

Functional benchmarking

Functional benchmarking tries to evaluate not only direct competitions performance but also the performance of other businesses operating in similar fields, solving problems that are relatable or performing comparable activities. It is easier to build benchmarking relationships or attain information when there is no direct competition between the two businesses. However, the outcome of the benchmarking process might not be as applicable from one industry to another, needing further investigation to be useful. (Metin Kozak, 29-30)

Relationship benchmarking

Relationship benchmarking refers to benchmarking performance with an associated organization, which the business already had an existing relationship with. When benchmarking against partners, it is easier to break down the confidentiality barriers and have access to complete information. (Metin Kozak, 29-30)

Overview of the benchmarking theory

Despite benchmarking being a useful tool for the company's product development, it can also be counterproductive when it's conducted subjectively, or the organization defaults into copying what other organizations are doing without throughout analysis. (Rowena Scott)

Numerous benchmarking methods have been proposed over time by different academics, researchers, and experts in the field. These methods define various amounts of required stages and phases for a benchmarking process. However, the connecting factor behind all the models is that they are fundamentally based on Deming's four stages: Plan, Do, Check, Act (PDCA). The main categorization of any benchmarking process can be presented with 4 different phases derived from the PDCA cycle: planning, data collection, analysis, and action.

The first step of a benchmarking process is identifying the areas and aspects that need to be measured. After these frames have been set, data collection methods should be determined, and data collected in a systematic manner. After the dataset has been gathered, it is analyzed to find key differences, strengths, and weaknesses between the compared subjects or to identify gaps in the organization's processes and product portfolio. Based on this analysis, the organization can decide on appropriate actions that need to be taken to achieve higher performance.

The traditional benchmarking implies that there is always a gap between the two measured aspects, the so-called gap analysis model. When analyzing the dataset, the highest positive value is considered as the best practice. When business A has a positive value compared to business B, it can be said that the measured aspect is a strength for business A and a weakness for business B. If a measured gap is large, it may indicate that the business on the negative side needs to rethink its approach radically.

An objective way to measure the performance difference between the two subjects is needed for the results to be insightful for an organization. In general, there are two main categories used to achieve accurate, non-subjective measurements. Both methods have their advantages and disadvantages, and these methods are often combined in benchmarking studies to reach the best results. (G. Anand, Rambabu Kodali)

Quantitative measurements

For a measure to be considered quantitative, it must fill the criteria of being numerically presentable in a uniform mathematical scale. This makes it a more appealing option for gap analysis, as there is no room left for interpretation, and it is certain that the achieved results are accurate. Using quantitative measurements simplifies the benchmarking process greatly, as it is much easier to identify the gaps between the measured areas. However, when performing a gap analysis, qualitative aspects should also be taken into consideration, as quantitative measures don't provide any insight into why the measured aspects are performing the way they do. Other aspects besides absolute numbers need to be measured to achieve good results. (Metin Kozak, 33-34)

Qualitative measurements

The goal of qualitative measurements is to collect data that is not directly quantifiable and doesn't have a uniform mathematical scale, but that can be assigned a soft number. To measure aspects such as quality or customer satisfaction, researchers often use Likert-type scales and percentage values to gather information about the organization's performance. These obtained values are not directly comparable with each other as they don't have a uniform scale, but it gives a good indication of how well the measured aspect is performing. (Metin Kozak, 33-34)

6 WORK

In future manufacturing systems, the degree of connectivity and mobility of the systems will be so high that relying on cable-based systems will not be possible. In general, wireless communication systems are a more effective way of transferring information compared to systems that require wiring between devices. In the past, wired solutions were preferable, as transmitters and receivers were expensive or not able to perform on a level required to ensure safe operation of the system. Now new technologies have made the devices more reliable, and the price of electronics has been greatly reduced, making wireless technology a viable option. However, when considering safety applications, the system must be able to perform with a very low risk of failure. The current problem with wireless safety systems are mainly related to transmission errors and reliable data transmission, as transmitting information over the radio is not as controllable or reliable as transmitting over a wired channel. The communication link can be experiencing difficulties for multiple different reasons:

- Physical objects in the signal path can result in loss or weakening of the communication link. This is especially problematic in industrial environments, as moving machines, vehicles, and equipment are common, which creates an additional layer of complexity.
- The interference caused by other devices can become problematic, especially if communicating at the 2.4GHz frequency band as it is used by many communication standards that have become commonplace in industrial environments. Interference can be dealt with to an extent, but the performance will most likely suffer if the whole operating area is not controlled. This will be even more crucial in the future as the number of wireless devices constantly increases.
- Weakened signal strength, which can result in the loss of transmitted packets
- Security issues are a concern, as the signals are transferred through a shared medium of open space, which is accessible by anyone. However, state-of-the-art encryption is very safe, practically unbreakable.
- The systems are getting larger, and they are increasingly networked with other systems, which results in more faults and errors as the number of connected objects increases within a system. This means that the control systems must be even more reliable in the future.

One solution to deal with the unpredictability of the communication channel is to use the black channel principle, where safety applications communicate through a non-safe communication channel. This channel is then monitored by an additional safety layer between the safety application and the communication system to find possible faults in the communication link, e.g., data corruption, unreceived messages, and unacceptable delays. This greatly simplifies the safety certification process, as the whole system doesn't have to be built from the safety standpoint. Another benefit is that regular communication channels can be used to transmit safety data. When using the black channel principle, the safety of the system is not dependent on the communication channel, but a good quality communication link is still desired as the loss of the communication link will initiate a machine shutdown, which results into increased machine downtime and production losses. In the white channel principle, all network components are subject to safety requirements, which means that everything related to the communication network must be safety certified. This includes routers, couplers, repeaters, interface converters, and all other network components. (Akerberg. J, Gidlund. M, Lennvall. T, Neander. J, Björkman. M: Efficient integration of secure and safety critical industrial wireless sensor networks)

Currently, the clear upside of using wired systems is the reliability of signal transmission, as the transferring medium is more secure, controllable, and with fewer disturbances. The reaction times over wire are also still in general superior to wireless systems. However, the wireless communication systems have made great advancements in recent years, with some almost reaching the performance of their wired counterparts with only a 10-fold difference in packet error rate and one to two milliseconds in latency. Even though wireless systems can't compete in terms of reliability yet, they have a higher potential for future applications. The main advantages of a wireless safety systems are:

- Flexibility as no cables are needed
- Reduced costs as the installation and maintenance of the system are easier
- Freedom of movement and improved work ergonomics
- Other possibilities, e.g., advanced diagnostics, control over mobile devices

One of the major benefits of wireless systems is their flexibility. Wireless safety devices allow the connection of remote machines and locations, where wiring would be expensive or impractical. For example, connecting moving machines and vehicles are difficult to achieve by using cable and highly expensive. When no wiring is required between the devices, installation, and maintenance of the system becomes simpler. In industry 4.0 era, the factory layouts are subject to rapid changes, and having the whole infrastructure

built on wireless devices enables quick layout changes and flexible adaptation to customer's needs. This reduces costs greatly, as changing the layout and retrofitting systems is made much simpler. Also, the possibility of wire damage is removed on the factory floor, and diagnostic information of the system is more readily available. Diagnostic data and operating actions can be displayed, for example, on a mobile device, which eases the task at hand. Even start, stop, and emergency stop functions can also be potentially initiated with a mobile phone in the future if the device is able to meet the safety requirements set by the standards.

During machine maintenance, set-up or inspection, it is often required for the personnel to enter the hazardous area even when the machine is still running on reduced speed. Traditional hardwired e-stops are sometimes not located within quick reach or in the safest possible location, and in some cases, the emergency at hand prevents moving to the e-stop station. In these situations, wireless safety devices perform better compared to wired safety systems, as the task can be carried out with greater freedom of movement, and the safety device is always within reach when needed. This also improves working ergonomics when the personnel are no longer hindered by heavy cables that are connected to the control device.

6.1 Chosen benchmarking criteria

As established before, product benchmarking, in general, involves 4 stages: planning, data collection, analysis, and action. The first step of this process was to create a comprehensive template where all the key information would be stored. The aspects that were picked for the comparison will be discussed in this chapter, as well as the reasons behind choosing them as the key attributes.

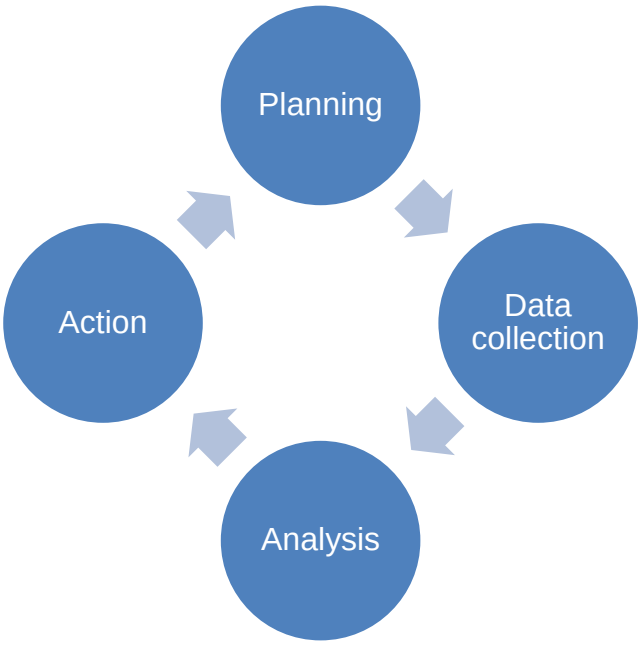


Figure 23. Product benchmarking process

For the comparison to be meaningful, only devices from the same ranges should be compared with each other, e.g., controller with another controller. Even if two devices from different ranges share the same function, it is not sensible to compare the two as they were developed with different applications in mind. For example, safety plc's have much greater performance, and flexibility compared to the regular safety controllers but are also considerably more expensive. In the comparison table, this information is presented in "System description" and "Product function" column.

Flexibility and diversity of the available safety functions are important factors. When a product can perform multiple functions at a time or has diversity in selectable safety functions, fewer devices are needed to build the whole safety chain. The possible safety functions are presented in the "safety functions" column.

The maximum transmission range is also important to consider, and it is displayed in the "transmission range" column. When the transmission range is smaller, either more devices are required to cover the whole operating area or movement with a control device will be restricted. The maximum operating range is dependent on multiple factors, e.g., environmental conditions, transmitter power, frequency. As transmitter power in most cases is adjustable and environmental conditions are application dependent, they weren't considered in this comparison, and the transmission ranges are given based on

the best-case scenario evaluated by the manufacturer. Operating frequency and frequency agility were also listed in the “frequency band” column.

One of the most crucial factors for overall safety is the time delay between the initial activation of the input device and the initiation of the output function. In an emergency, every millisecond counts, and wireless communication systems are still not able to compete with wired systems when it comes to reaction times.

Key requirements for future manufacturing systems are the ease of system integration, installation, and expansion. Keeping the overall system as simple as possible while still being effective is also desirable, as it is easier to manage. The number of safe inputs and outputs combined with diagnostic outputs describes how many safe channels are supported by one individual device, and the capability to give out diagnostic information. The highest number of linked devices is presented in the “maximum configuration” column.

The safety values describe the system's reliability according to standard ISO13849-1. Depending on the application, different requirements are set for safety based on the risk evaluation of the system. The required safety level is application dependent, and in general, devices are designed to comply with the typical requirements set by the given application. In general, the safer the device is, the better, but there is always a trade-off between reliability and price. The reliability aspects are described in “PFHD,” “MTTFD,” “Cat.,” and “PL” columns.

The physical features are also an important factor to consider. When there is limited space available, the compactness of the product is important. For controlling devices that must be carried for long periods of time, the weight of the device, dimensions, and attachability are important, e.g., emergency stop that can be strapped to waist is ergonomically better than a handheld button. The protection class defines if the device is suitable to be operated in a certain environment. Devices that can tolerate harsher conditions are more expensive, so usually, multiple options of the same device are on the market with different protection classes. These aspects are covered by multiple columns at the end of the table.

Finally, any relevant information of the system that didn’t fit into the above categories is concluded in the “notes” column.

6.2 Benchmarking table summary

Note: benchmarking table confidentialThe most common wireless safety devices found on the market are E-stops and controlling buttons/enabling devices. This is most likely explained by the high demand of these devices, as well as having the biggest upside of having them available wirelessly. Having static input devices operate wirelessly doesn't have as much of an impact on device usability as mobile input devices, and having the whole infrastructure built wireless has benefits mainly regarding installation, retrofitting, and maintenance.

The most popular used frequency bands are located around 400MHz and 800MHz ISM bands. The reason that these frequencies are often preferred in safety applications is simply that the channel is subject to less interference, since most devices operate at the 2.4GHz ISM band, and the transmission range is also longer at these frequencies. For most devices, a typical transmission range is around 100 meters under industrial ambient conditions. The transmission range can change radically between different applications since the operating environment has a huge effect, and usually, there is no line-of-sight between the two communicating devices. In a difficult environment with a high number of obstacles and interference, the devices are not able to reach the evaluated 100m range, and in some cases, a line-of-sight connection can reach up to 2km. Almost all of the listed devices support frequency hopping and configuring the transmitting bandwidth, so that the device remains operational even if it is experiencing heavy interference.

The black channel principle is applied by most manufacturers, as wireless communication in most cases is not robust enough to be used in safety applications without an additional safety layer that monitors the communication channel. Additionally, to improve the communication links quality, some of the listed technologies support changing the desired receiver from the control device, or apply device roaming, where the remote controller can self-configure the best signal route and change between stations when moving from one point to another. This has an additional benefit when considering the usability of the device.

Regarding device performance, the devices can reach almost the same safety values as their wired counterparts. This is mainly achieved by the fact that the communication channel doesn't influence the device reliability, as an additional safety layer is established between the safety application and the communication channel. This has a

marginally negative impact on the whole system's reliability, as more complexity is introduced to the system. However, as the communication channel is not as stable as a wired channel, and the safety of the system is ensured by initiating a stop when the communication link is lost, machine downtime will be increased. To ensure that the operator is in safe area on machine start-up, most applications require infra-red connection between the devices before start is initiated.

7 CONCLUSION

Wireless systems offer many advantages over wired systems, and as organizations are getting ready for the new era of manufacturing the pressure to go wireless increases. When no wires are needed between the communicating entities, the system becomes more flexible and easier to manage, which results in reduced costs and improved performance. In wireless safety applications, reliability and timeliness of the transmission are the main requirements set for the system. When the transmission medium is not controlled, and the signals propagate freely in open space, a new set of problems is introduced to the system, especially in industrial environments. Many factors that are beyond the systems control, e.g., interferences, objects in the signal path, and environmental conditions can negatively influence the communication channels quality.

The goal of this work was to create an easily comprehensible overview of the current state of wireless safety technology. One of the most efficient ways of establishing a clear overview is to perform product benchmarking, and this approach was chosen for this work. Since these products are from direct competitors, the model of competitive benchmarking was applied. As established in the benchmarking chapter, finding information about the company's direct competition is often extremely challenging, as both organizations are competing for the same customer base. This naturally means that only the customer relevant information of the product is public, and other information of the product is kept confidential. This makes it difficult to establish a deep level analysis of the products at hand. In this work, the focus was on analyzing the specifications and aspects that are, in most cases, publicly available and of core importance to the functionality of the product.

The investigated wireless safety devices could reach the performance of their wired counterparts when measured purely based on the reliability values of the safety function, but as the wireless channel is not as stable as a wired channel, machine shutdowns will be initiated more frequently as a cause of lost communication link. This will naturally increase machine downtime, which will result in lost production time. A suitable wireless alternative system design can be achieved in most cases by careful design and by factoring in all the limitations that are present. There are viable wireless safety products on the market, and the need for wireless safety products will increase in the future. However,

to fully harness the benefits of wireless communication in safety applications, new novel solutions, and advances in reliable real-time communication are still needed.

BIBLIOGRAPHY

Company profile, [Referred 26.04.2019]. (https://www.schneider-electric.us/en/about-us/company-profile/)

Muhuri P. K. & Shukla. A. K. & Abraham A. Industry 4.0: A bibliometric analysis and detailed overview, Engineering Applications of Artificial Intelligence 78 (2019) 218–235

Collin, J. & Saarelainen, A. 2016. Teollinen Internet. Helsinki: Talentum.

Chou S. The fourth industrial revolution: Digital fusion with internet of things, Journal of International Affairs. Fall/Winter2018, Vol. 72 Issue 1, p107-120.

Siirilä T. 2008 Koneturvallisuus: EU-määräysten mukainen koneiden turvallisuus

Siirilä T. 2008 Koneturvallisuus: EU:n direktiivien ja standardien soveltaminen käytännössä

Siirilä T. 2009 Koneturvallisuus: Ohjausjärjestelmät ja turvalaitteet

Machine safety guide, Schneider Electric (https://download.schneider-electric.com/files?p_enDocType=Brochure&p_File_Name=dia4ed1100102en%28web%29.pdf&p_Doc_Ref=DIA4ED1100102EN)

Schneider Electric 2018, Machine_Safety_June_2018. [PowerPoint-presentation]. [Referred 15.05.2019]. Available: Only for internal use.

Machine safety guide, SICK (https://cdn.sick.com/media/docs/8/78/678/Special_information_Guide_for_Safe_Machinery_en_IM0014678.PDF)

Schiller J. 2003, Mobile communications

Pepperl-fuchs, Wireless safety guide (https://files.pepperl-fuchs.com/webcat/navi/productInfo/doct/tdoct1933b_eng.pdf?v=20130903000000)

Raúl Rondó, Mikael Gidlund, Krister Landernäs Evaluating Bluetooth Low Energy Suitability for Time-Critical Industrial IoT Applications

Schneider Electric. 2018. 01 Machine_Safety_June_2018. [PowerPoint-presentation]. Schneider Electric [Referred 14.06.2019]. Available: Only for internal use.

Quan Wang ; Jin Jiang, Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards. IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 3, thirdquarter 2016, p2197-2219)

Rowena Scott Benchmarking: A Literature Review 2015

Metin Kozak: Destination Benchmarking: Concepts, Practices and Operations

G. Anand, Rambabu Kodali, Benchmarking the benchmarking models

Wireless Safety: Massive Kooperation macht Echtzeit möglich (https://www.git-sicherheit.de/topstories/security/wireless-safety-massive-kooperation-macht-echtzeit-moeglich) [Referred 14.05.2019].

Etsi, radio technologies (https://www.etsi.org/technologies/radio/) [Referred 08.05.2019].

Bluetooth Low Energy (LE) (https://www.bluetooth.com/bluetooth-technology/radio-versions/) [Referred 18.06.2019].

Control, The Hidden Network (https://www.controlglobal.com/articles/2011/HiddenNetwork1102/) [Referred 14.06.2019].

Elcio Carlos do Rosario ; Rodrigues Joel J. P. C.Wireless Sensor Networks in Industry 4.0: WirelessHART and ISA100.11a

What is Zigbee? (https://zigbeealliance.org/solution/zigbee/) [Referred 04.05.2019].

Echoring, wireless propagation effects and their impact on reliable transmissions (https://echoring.com/wireless-propagation-effects-and-their-impact-on-reliable-transmissions/) [Referred 13.06.2019].

ISA 100, Universal Industrial Wireless Network (https://isa100wci.org/en-US/About-ISA100-Wireless/Universal-Industrial-Wireless-Network) [Referred 10.06.2019].

Akerberg. J, Gidlund. M, Lennvall. T, Neander. J, Björkman. M: Efficient integration of secure and safety critical industrial wireless sensor networks